| FORM PTO-1390 (REV. 5-93) | U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE | ATTORNEY'S DOCKET NUMBER 2345/97 |
|---|---|---|

**TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371**

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/403689

| INTERNATIONAL APPLICATION NO. | INTERNATIONAL FILING DATE | PRIORITY DATE CLAIMED: |
|---|---|---|
| PCT/EP98/01391 | 11.03.98 (11 March 1998) | 22.04.97 (22 April 1997) |

TITLE OF INVENTION
ENCRYPTION METHOD AND DEVICE

APPLICANT(S) FOR DO/EO/US
KOWALSKI, Bernd and WOLFENSETETTER, Klaus-Dieter

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

**Items 11. to 16. below concern other document(s) or information included:**

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: Preliminary Examination Report and International Search Report.

EXPRESS MAIL NO. EL179668975US

514 Rec'd PCT/PTO 22 OCT 1999

| U.S. APPLICATION NO. (If known, see 37 C.F.R.1.5) 09/403689 | INTERNATIONAL APPLICATION NO. PCT/DE98/01391 | ATTORNEY'S DOCKET NUMBER 2345/97 |
|---|---|---|

| 17. ☒ The following fees are submitted: | CALCULATIONS | PTO USE ONLY |
|---|---|---|
| **Basic National Fee (37 CFR 1.492(a)(1)-(5)):** Search Report has been prepared by the EPO or JPO . . . . . $840.00 | | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) . . . $670.00 | | |
| No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) . . . . . $760.00 | | |
| Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO . . . . . $970.00 | | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) . . . . . $96.00 | | |
| **ENTER APPROPRIATE BASIC FEE AMOUNT =** | $ 840 | |
| Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)). | $ | |

| Claims | Number Filed | Number Extra | Rate | | |
|---|---|---|---|---|---|
| Total Claims | 11 - 20 = | 0 | X $18.00 | $ 0 | |
| Independent Claims | 3 - 3 = | 0 | X $78.00 | $ 0 | |
| Multiple dependent claim(s) (if applicable) | | | + $260.00 | $ 0 | |
| | | | **TOTAL OF ABOVE CALCULATIONS =** | $ 840 | |
| Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28). | | | | $ | |
| | | | **SUBTOTAL =** | $ 840 | |
| Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). + | | | | $ | |
| | | | **TOTAL NATIONAL FEE =** | $ 840 | |
| Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property + | | | | $ | |
| | | | **TOTAL FEES ENCLOSED =** | $ 840 | |
| | | | Amount to be: refunded | $ | |
| | | | charged | $ | |

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of **$840.00** to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

**NOTE:** Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

By: Reg No 35,952

SIGNATURE

SEND ALL CORRESPONDENCE TO:

Kenyon & Kenyon
One Broadway
New York, New York 10004

Richard L. Mayer, Reg. No. 22,490
NAME

10/22/99
DATE

228879

[2345/97]

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| Inventors | : | Bernd KOWALSKI et al. |
| Serial No. | : | To Be Assigned |
| Filed | : | Herewith |
| For | : | ENCRYPTION METHOD AND DEVICE |
| Examiner | : | To Be Assigned |
| Art Unit | : | To Be Assigned |

Assistant Commissioner for Patents
Washington, D.C. 20231

**PRELIMINARY AMENDMENT**

SIR:

Kindly amend the above-identified application before examination, as set forth below.

**IN THE SPECIFICATION:**

Please amend the specification as follows:

On page 1, before line 1, insert:

--FIELD OF THE INVENTION--.

On page 1, line 1, before "invention", insert --present--.

On page 1, delete lines 2-4, and insert:

--device for implementing the method.--.

On page 1, before line 6, insert:

--BACKGROUND INFORMATION--.

EL179668975US

On page 2, before line 18, insert:

--SUMMARY OF THE INVENTION--.

On page 2, line 18, replace "The" with --An--.

On page 2, line 19, replace "the" with --an--.

On page 2, delete lines 26-35.

On page 3, delete lines 1-4.

On page 3, line 6, replace "The great" with --An--.

On page 3, line 7, before "invention", insert --present--, and replace "can always" with --may--.

On page 3, line 8, replace "such as" with --e.g.,--.

On page 3, line 10, after "(", insert --e.g., a--.

On page 3, line 20, replace "example" with --example,--.

On page 3, line 29, replace "All the complex" with --Complex--.

On page 3, line 31, delete "proposed,".

On page 3, line 33, replace "card" with --card, for example--.

On page 3, line 35, replace "example" with --example,--.

On page 4, line 1, replace "is" with --may be--.

On page 4, line 2, replace "as" with --as, for example,--.

On page 4, delete lines 7-32, and insert:

--BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a Vernam cipher according to the present invention.

Fig. 2 illustrates a symmetrical cipher according to the present invention.

Fig. 3 illustrates a first embodiment according to the present invention using an asymmetrical cipher.

Fig. 4 illustrates an second embodiment according to the present invention using a Vernam cipher.

Fig. 5 illustrates a third embodiment according to the present invention using a Vernam cipher.

Fig. 6 illustrates a fourth embodiment according to the present invention using a crypto-module.

Fig. 7 illustrates a fifth embodiment according to the present invention using the crypto-module.--.

On page 4, before line 35, insert:

--DETAILED DESCRIPTION--.

On page 5, line 2, replace "as" with --as, for example,--.

On page 5, line 4, replace "The" with --A--.

On page 5, line 5, delete "of such known methods".

On page 5, line 7, replace "composed" with --including--.

On page 5, line 12, replace "as" with --as, for example,--.

On page 5, line 14, replace "usually" with --typically--.

On page 5, line 20, replace "example" with --example,--.

On page 5, line 25, replace "example" with --example,--.

On page 5, line 31, replace "required" with --used--.

On page 6, line 9, replace "example" with --example,--.

On page 6, line 10, replace "example" with --example,--.

On page 6, line 28, replace "The" with --An--.

On page 6, line 29, replace "7 and Fig. 8" with --6 and Fig. 7--.

On page 6, line 30, delete "typical".

On page 6, line 32, replace "composed" with --including, for example,--.

On page 7, line 4, replace "as" with --as, for example,--.

On page 7, line 15, replace "The" with --An--.

On page 7, line 26, replace "example" with --example,--.

On page 8, line 4, delete "proposed,".

On page 8, line 5, replace "as" with --as, for example,--.

On page 8, line 7, replace "example" with --example,--.

On page 8, line 26, replace "example" with --example,--.

On page 8, line 33, replace "example" with --example,--.

On page 8, delete line 1, and insert:

--WHAT IS CLAIMED IS:--.

**IN THE ABSTRACT:**

Please amend the Abstract, as follows:

Delete line 1, and insert:

-- Abstract Of The Disclosure--.

Line 3, replace "proposed" with --disclosed--.

Line 5, replace "encryptor" with --encryptor. The encryptor may be--.

Line 11, after "(", insert --e.g.,--.

Line 13, delete "(PC)".

Line 15, replace "such as" with --e.g.,--.

Line 18, delete "(KV)".

**IN THE CLAIMS:**

Please cancel claims 1-7 without prejudice.

Please add the following new claims:

8. (New) A method for implementing an encryption system, comprising the steps of:

generating a Vernam key via a symmetrical cipher, the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length;

encrypting, via a Vernam key, the message using logic operations of a Vernam cipher;

communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher;

regenerating the Vernam key; and

decrypting the message using the regenerated Vernam key.

9. (New) The method according to claim 8, wherein the encryption system uses a Vernam cipher.

10. (New) The method according to claim 9, wherein the Vernam cipher is a very simple mathematical operation.

11. (New) The method according to claim 10, wherein the very simple mathematical operation is EXOR.

12. (New) The method according to claim 8, further comprising the steps of:

installing a symmetrical cipher and a storage space in a crypto-module, the storage space storing the Vernam key, the crypto-module being separate from an encryptor, the encryptor including at least one of a chip card, a multifunctional PC interface adapter and a PCMCIA module; and

performing Vernam cipher operations exclusively in the encryptor.

13. (New) The method according to claim 8, further comprising the steps of:

implementing the asymmetrical cipher and a storage space in an external crypto-module, the external crypto-module being separate from the encryptor; and

controlling, via the Vernam cipher, encryption operations in the encryptor.

14. (New) The method according to claim 8, wherein the Vernam key is stored in an encryptor.

15. (New) An encryption system, comprising:

means for generating a Vernam key via a symmetrical cipher, the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length;

means for encrypting, via a Vernam key, the message using logic operations of a Vernam cipher;

means for communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher;

means for regenerating the Vernam key;

means for decrypting the message using the regenerated Vernam key;

crypto-hardware including at least one of a chipcard and a multifunctional PC interface adapter with built-in special crypto-hardware; and

the encryptor being capable of coupling to the crypto-hardware, the encryptor including at least one of a personal computer, software and a terminal which implements a Vernam cipher for broad-band applications in software.

16. (New) The encryption system according to claim 15, wherein the crypto-hardware is designed as an external crypto-module and wherein the crypto-hardware has an intermediate storage, the intermediate storage storing reserve storage of the Vernam key.

17. (New) The encryption system according to claim 16, wherein the intermediate storage is disposed in one of the personal computer and the terminal.

18. (New) An encryption system, comprising:

a secret key having a defined key length;

a variable parameter having a length which is a function of the defined key length;

a symmetrical cipher;

a Vernam key having a length that is equal to a length of a message to be protected; the Vernam key being generating via the symmetrical cipher with aid from the secret key and the variable parameter, the Vernam key encrypting the message using logic operations from a Vernam cipher; and

at least one of a message-transmission path and a secure channel, the message-transmission path being a path over which the encrypted message is communicated, the message-transmission path being secured via an asymmetrical cipher, the secure channel being separate from the message-transmission path,

wherein the secret key and the variable parameter are communicated over at least one of the message-transmission path and the secure channel and, subsequently, used in regenerating the Vernam key, the regenerated Vernam key decrypting the message.

## Remarks

This Preliminary Amendment cancels, without prejudice, claims 1-7 in the underlying PCT Application No. PCT/EP98/01391. This Preliminary Amendment further adds new claims 8-18. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

The above amendments to the specification and abstract conform the specification and abstract to U.S. Patent and Trademark Office rules, and do not introduce new matter into the application.

The underlying PCT Application No. PCT/EP98/01391 includes an International Search Report dated September 8, 1998. The International Search Report includes a list of documents that were uncovered in the underlying PCT Application. A copy of the International Search Report is included herewith. Also enclosed is a translation of the International Search Report.

The underlying PCT Application also includes an International Preliminary Examination Report dated August 30, 1999. A copy of the International Preliminary Examination Report is included herewith. Also enclosed is a translation of the International Preliminary Examination Report.

It is respectfully submitted that the subject matter of the present application is new, non-obvious, and useful. Prompt consideration and allowance of the application are respectfully requested.

Respectfully submitted,

Richard L. Mayer

Dated: 10/22/99

By: Mary C. Werner Reg No 30,333
Richard L. Mayer
Reg. No. 22,490

KENYON & KENYON
One Broadway
New York, NY 10004
(212) 425-7200

228612

[2345/97]

# ENCRYPTION METHOD AND DEVICE

The invention relates to a method for encryption and to a device for implementing the method according to the precharacterizing portion of Claim 1 and Claim 5, respectively.

Modern encryption methods are being increasingly employed in information processing and telecommunication engineering. However, the use of encryption methods and corresponding devices is persistently impeded by the below-described problems and factors, although mass proliferation, particularly in the multimedia sector and in the field of information processing, calls for a very high standard of security:

- The encryption of broad-band signals requires the installation of costly crypto-hardware in personal computers and terminals. The currently available low-cost crypto-chipcards operate only at a low throughput rate of significantly less than 100 kbit/s.

- Encryption methods are often protected by property rights and not internationally standardized, so that no low-cost mass products with integrated crypto-hardware are available.

- For reasons of cost, crypto-hardware for broad-band encryption frequently employs just one encryption method. Consequently, the personal computers and other terminals equipped with one of these methods are not able to support any number of encryption

methods. This results in a great restriction in the compatibility of the indicated devices.

- Crypto-hardware is subject to strict international trade restrictions, with the result that the export, for example, of encryption terminals is very greatly restricted, which is why the use of such devices is very greatly limited and the prices for these devices are very high.

The book by Alfred Beutelspacher: *"Kryptologie"*, Vieweg Verlag, 1993, describes and presents encryption methods such as the Vernam cipher. In addition, encryption methods such as the RSA method are described in ITU/CCITT Recommendations X.509 and in CACM Communications of the ACM, Vol. 21, No. 2. pp. 120-126, 1978.

The object of the present invention is to create a method and a device for encryption, the aim being to realize simplified implementation while avoiding expensive and incompatible broad-band encryption hardware, so that in the future, low-cost mass products can be equipped with integrated crypto-hardware, this considerably improving the standard of security of such products.

The design approach of the present invention for the method is characterized in the characterizing part of Claim 1.

Further embodiments or refinements of the method according to the invention are disclosed in the characterizing parts of Claims 2 through 4.

The design approach for implementing the encryption

methods and the device, respectively, is characterized in the characterizing part of Claim 5. Further refinements of the device are characterized in the characterizing parts of claims 6 and 7.

The great advantage of the design approach according to the invention is that the encryptors can always operate with the same Vernam cipher (such as EXOR). They can be used without problem even when the external crypto- or PCMCIA modules (multifunctional PC interface adapter) employ different symmetrical and asymmetrical ciphers. The Vernam cipher can also be implemented in software for high throughput rates, so that all encryptors are able to get along without the need for expensive crypto-hardware and can be used cost-effectively in mass products because their manufacture is technologically simple. The external crypto-modules likewise remain competitively priced because the Vernam key, produced in reserve, can also be generated by a low-performance or low-speed chipcard, for example for reserve in the Vernam-key storage, without slowing down the actual broad-band encryption process operating independently thereof.

Because of the method described herein, the encryptors are freed from the problems of expensive, high-performance and mutually incompatible crypto-hardware. By contrast, the Vernam cipher can be implemented very simply and cost-effectively in software, and consequently by storage. All the complex crypto-functions are located outside of the encryptor. They are interchangeable by module and can be implemented in the proposed, competitively priced and low-speed external crypto-modules, such as the chipcard or the PCMCIA card. The methods used are negotiated or "signaled" during coordination between sender and receiver, for example on

the transmission path. The encryptor itself is composed merely of software, such as PC software or any other terminal/information system with an integrated Vernam cipher which does not need to be supported by expensive crypto-hardware for the actual encryption process.

Following, the invention is described in greater detail with reference to exemplary embodiments shown in principle in the drawing, in which:

Fig. 1 shows a known Vernam cipher represented in simplified form;

Fig. 2 shows a modern, known symmetrical cipher;

Fig. 3 shows a configuration with the additional use of an asymmetrical cipher;

Fig. 4 shows a configuration with Vernam cipher;

Fig. 5 shows a further version with Vernam cipher;

Fig. 6 shows a configuration with external crypto-module; and

Fig. 7 shows a further configuration with crypto-module.

The reference characters/abbreviations used in the appended list are employed in the Drawing, in the following description, in the Patent Claims and in the Abstract.

Fig. 1 shows a Vernam cipher in simplified form. The

encryption process, identified here by "V", may be a very simple mathematical operation, such as EXOR, which also allows broad-band encryption in software, i.e., without the support of a special crypto-hardware. The disadvantage of such known methods, however, is that the message, indicated by "TEXT", must be encrypted using a Vernam key KV composed of a random number having the length of the message to be encrypted. Consequently, long Vernam keys are required for long messages. This means that the Vernam cipher can only be used to a limited extent for practical applications. Fig. 2 shows a modern symmetrical cipher S, such as DES or IDEA, which also still provides excellent security in the case of relatively short key lengths, usually 128 bits for the secret symmetrical key KS. DES and IDEA, respectively, are data encryption standards (ANSI and ASCOM) ISO 9979. Here too, however, as in the case of the Vernam cipher, the secret key KS required for encryption and decryption must be exchanged via a secure channel, independent of the transmission path used for the message, for example with the aid of a courier. The configuration shown in Fig. 3, which is described in detail in the literature source indicated in the introduction, has avoided this disadvantage through the additional use of an asymmetrical cipher A, for example the RSA method, for the transmission of the secret encryption key KS. In this case, the encryption key KS is encrypted with the public asymmetrical key KAp of the recipient and can subsequently be decrypted again by the recipient using his secret symmetrical key. The public recipient key KAp required for this purpose at the sender's end can be transmitted to him by the recipient over any insecure channel. Of course, the message could also be encrypted directly with the public recipient key KAp, but the

achievable performance of the hardware and software available for an asymmetrical cipher is significantly lower than in the case of a symmetrical cipher, so that in the case of long messages and to attain a high processing speed, use is made of the asymmetrical and symmetrical ciphers, usually in the combination shown in Fig. 3, namely a hybrid method. In Fig. 4, the encryption of a secret parameter IV of variable length, for example n · 180 bits, with a symmetrical key KS, for example 128 bits, results in the generation of a very long (pseudo)-random number which, as Vernam key KV, finally encrypts the message to be protected. For transmission of the encryption/ decryption key to the recipient, however, the courier in this case does not need to transport the Vernam key KV, but merely the key KS and the parameter IV, from which the Vernam key KV can easily be simulated on the recipient's side, because the same configuration exists here as on the sender's side. Fig. 5 shows encryption using combined asymmetrical, symmetrical and Vernam ciphers, as in Fig. 4. In contrast to Fig. 4, which requires a courier for exchanging the secret key information, according to Fig. 5 an asymmetrical cipher is used for this purpose, analogous to Fig. 3. The public recipient key KAp is fed in on the sender's side and the asymmetrical sender key KAs on the recipient's side.

The advantage of this procedure is made apparent in Fig. 7 and Fig. 8. The upper halves of Fig. 6 and Fig. 7, therefore, each show two typical terminal configurations. The gray-shaded elements represent the external crypto-hardware, composed either of a chipcard or of a multifunctional PC interface adapter or PCMCIA module with built-in special crypto-hardware or a built-in

special chipcard. The encryptor, on the other hand, is implemented as a conventional PC, with software or another terminal which, however, with the exception of the very simple Vernam cipher, such as EXOR, that can be implemented even for broad-band applications in software, requires no further crypto-technology. Fig. 6 and Fig. 7 both show that the external crypto-modules are capable of taking on all the complex crypto-functions, generating the Vernam key KV, so to speak, as reserves and storing them in a suitable intermediate storage, the KV storage, until they are gradually used up by the encryption process through the logic operations V. The KV storage may be installed either in the personal computer or terminal, or also in the crypto-module in the form of a chipcard or PCMCIA module. The advantage of the devices according to Fig. 6 and Fig. 7 is that the encryptor is always able to operate with the same Vernam cipher, even if the external crypto- or PCMCIA modules use different symmetrical and asymmetrical ciphers. The Vernam cipher can also be implemented in software for high throughput rates, so that all encryptors are able to get along without expensive crypto-hardware and can be mass-produced at low cost. The external crypto-modules likewise remain competitively priced because the Vernam key, produced in reserve, can also be generated by a low-performance, i.e., low-speed chipcard, for example for reserve in the KV storage, without slowing down the actual broad-band encryption process which operates independently thereof.

Because of the method described herein, the encryptors are freed from the problems of expensive, high-performance and mutually incompatible crypto-hardware. On the other hand, the Vernam cipher can be implemented very simply and inexpensively in software. All the

complex crypto-functions are located outside of the encryptor. The great advantage is also that they are interchangeable by module and can be implemented in the proposed, competitively priced and low-speed external crypto-modules, such as a chipcard or a PCMCIA card. The methods used are negotiated or signaled during coordination between sender and receiver, for example on the transmission path.

The method for the low-cost implementation even of high-performance encryption functions in an encryptor which may be composed merely of PC software or any other terminal/information system with integrated Vernam cipher that does not need to be supported by expensive crypto-hardware for the actual encryption process has the distinction that, with the aid of a secret key KS having a defined key length and using a variable parameter having a defined bit length, a Vernam key KV having the length of the message to be encrypted is generated by way of any symmetrical cipher S, the Vernam key KV, on its part, encrypting the message to be protected by way of the Vernam cipher, the secret key KS and the parameter IV being communicated from the sender to the recipient either via a secure channel separate from the message-transmission path, or directly on the message-transmission path, for example secured by an asymmetrical method A, the recipient regenerating the Vernam key KV using the above-described method in order to be able therewith to decrypt the received message. The symmetrical and, optionally, also the asymmetrical cipher and, optionally, also the storage for the Vernam key, namely the KV storage, are accommodated in an external crypto-module separate from the encryptor, for example in the form of a chipcard or PCMCIA module or the like,

while only the Vernam cipher and, optionally, the storage KV for the Vernam key remain in the encryptor.

List of reference characters

| | |
|---|---|
| KV | Vernam key |
| V | Logic operation, such as EXOR |
| KS | Secret symmetrical key |
| S | Symmetrical cipher, such as IDEA |
| KAp | Recipient key (asymmetrical) |
| KAs | Sender key (asymmetrical) |
| A | Asymmetrical cipher |
| IV | Secret variable parameter |
| PCMCIA | Multifunctional PC interface adapter |
| PC-SW | PC software |

Patent Claims

1. A method for the simplified implementation of encryption methods, particularly the Vernam cipher, where the encryption process may be a very simple mathematical operation, such as EXOR, characterized in that

- with the aid of a secret key (KS) having a defined key length (x bits) and using an optionally variable parameter (IV) having a length of n · x bits, a Vernam key (KV) having the length of the message to be encrypted is generated by way of any symmetrical cipher (S);

- using logic operations of the Vernam cipher (V), the Vernam key (KV) encrypts the message to be protected;

- the secret key (KS) and the parameter (IV) are communicated from the sender to the recipient via a secure channel separate from the message-transmission path or directly on the message-transmission path, secured by an asymmetrical method (A) or the like; and

- the recipient regenerates the Vernam key (KV) and therewith decrypts the received message.

2. The method as recited in claim 1, characterized in that

- the symmetrical cipher and the storage for the Vernam key (KV) are installed in a crypto-module, separate from the encryptor, in the form of a

chipcard, a multifunctional PC interface adapter or module (PCMCIA); and

- only the Vernam cipher operations are performed in the encryptor.

3. The method as recited in claim 1, characterized in that

- the asymmetrical cipher and the storage for the Vernam key (KV) are implemented in an external crypto-module separate from the encryptor; and

- the Vernam cipher controls the encryption operations in the encryptor.

4. The method as recited in one of claims 1 through 3, characterized in that the Vernam key (KV) is stored in the encryptor.

5. A device for implementing the methods as recited in one of claims 1 through 4, characterized in that

- the crypto-hardware is composed of a chipcard or a multifunctional PC interface adapter (PCMCIA module) or the like, with built-in special crypto-hardware; and

- the encryptor is made of a conventional personal computer or the like, software or another terminal which implements a very simple Vernam cipher for broad-band applications in software

6. The device according to one of the methods as recited in claims 1 through 4, characterized in that the crypto-

hardware is designed as an external crypto-module and has an intermediate storage for the reserve storage of the Vernam key (KV).

7. The device as recited in one of claims 6 and 7, characterized in that the storage for storing the Vernam key (KV) is disposed either in the personal computer (PC) or in another terminal.

Abstract of the Disclosure

A method and a device are proposed for the low-cost implementation even of high-performance encryption functions in an encryptor composed merely of PC software or the like, or of any other terminal/ information system with integrated Vernam cipher which does not need to be supported by expensive crypto-hardware for the actual encryption process. The crypto-hardware is made either of a chipcard or a multifunctional PC interface adapter (PCMCIA module) with built-in special crypto-hardware. The encryptor, on the other hand, is a conventional personal computer (PC), software or another terminal which, however, with the exception of the very simple Vernam cipher (such as EXOR), needs no further crypto-technology even for broad-band applications in software. The external crypto-modules contain all the complex crypto-functions which generate the Vernam key (KV) in reserve, the reserves being temporarily stored in an intermediate storage until they are gradually used up by the encryption process through logic operations of the method. The storage may be installed either in the PC or terminal, or also in the crypto-module. The encryptor always operates with the same Vernam cipher, even if the external crypto- or PCMCIA modules use different symmetrical and asymmetrical ciphers. External crypto-modules in the form of chipcards or PCMCIA modules are inexpensive to manufacture. All the complex crypto-functions are located outside of the encryptor. They are interchangeable by module and can be implemented in the proposed low-cost and somewhat lower-speed external crypto-modules.

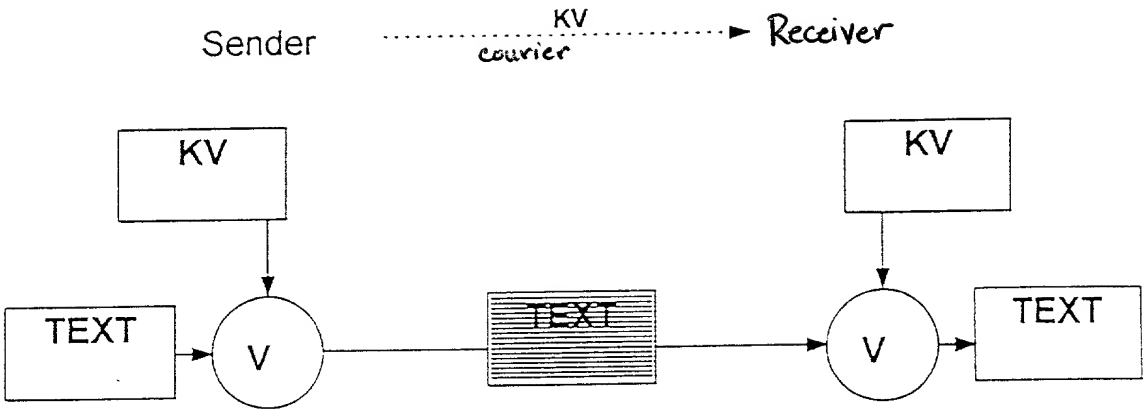

Sender
KV
courier
Receiver
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 1

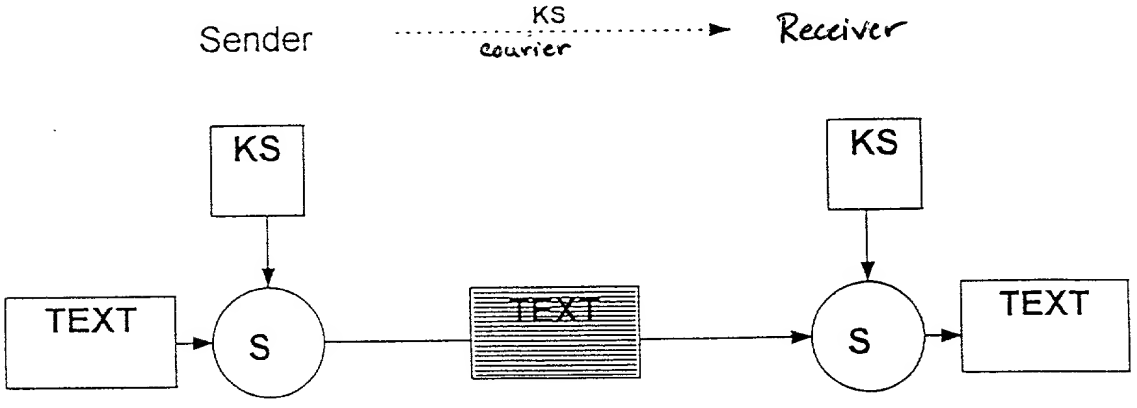

Sender
KS
courier
Receiver
KS
KS
TEXT
S
TEXT
S
TEXT

FIG. 2

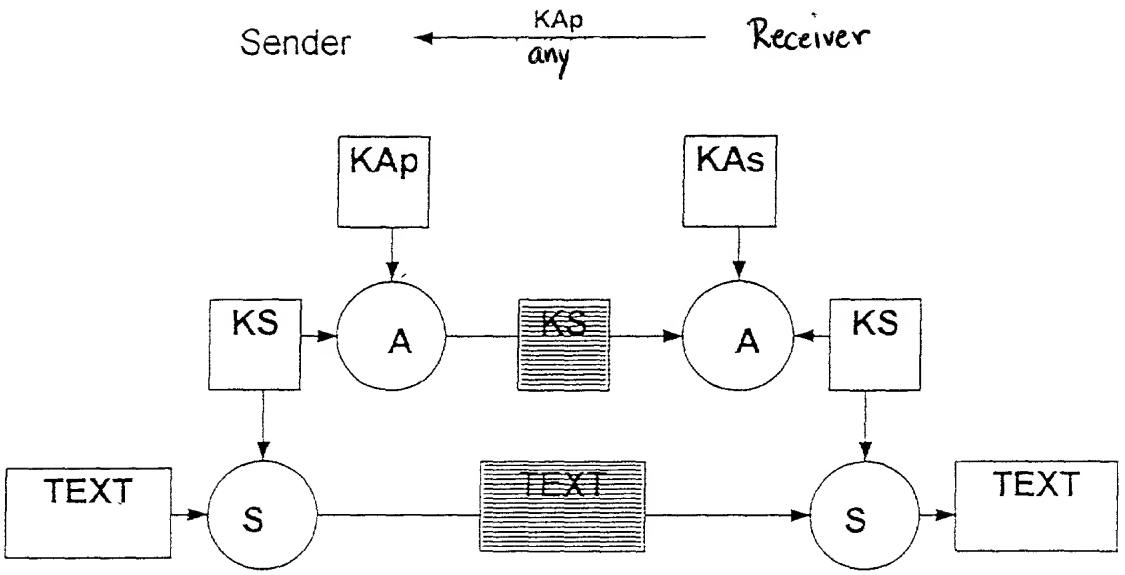

Sender
KAp
any
Receiver
KAp
KAs
KS
A
KS
A
KS
TEXT
S
TEXT
S
TEXT

FIG. 3

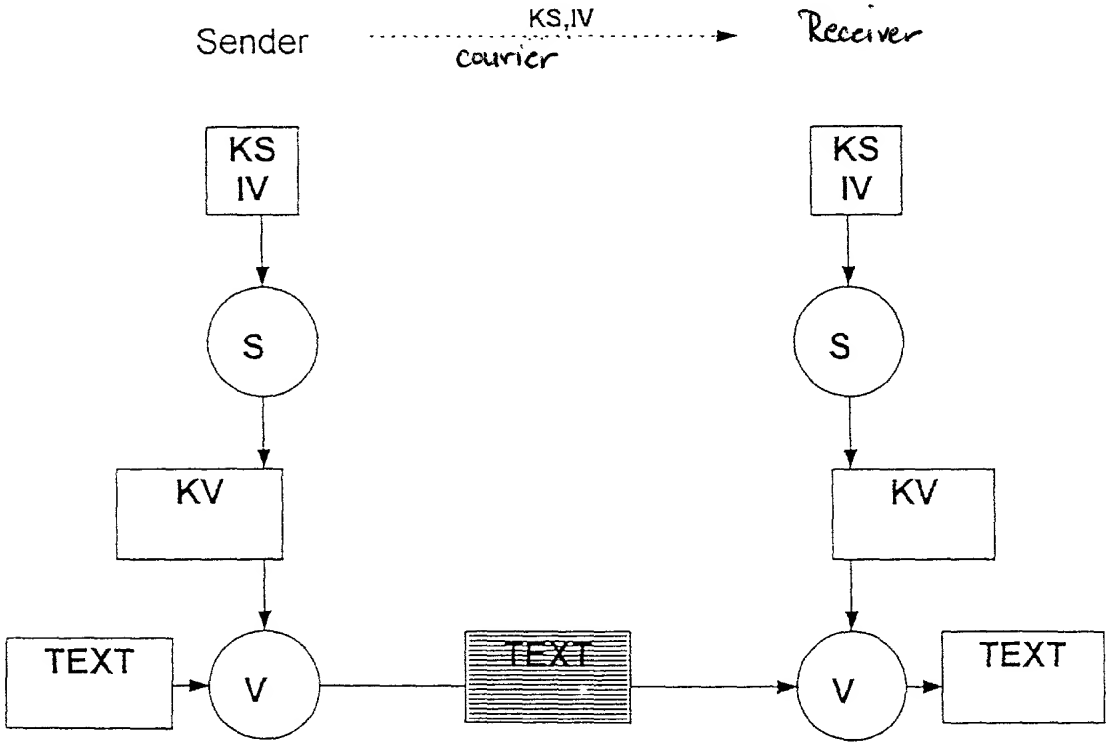

Sender
KS,IV
courier
Receiver
KS
IV
KS
IV
S
S
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 4

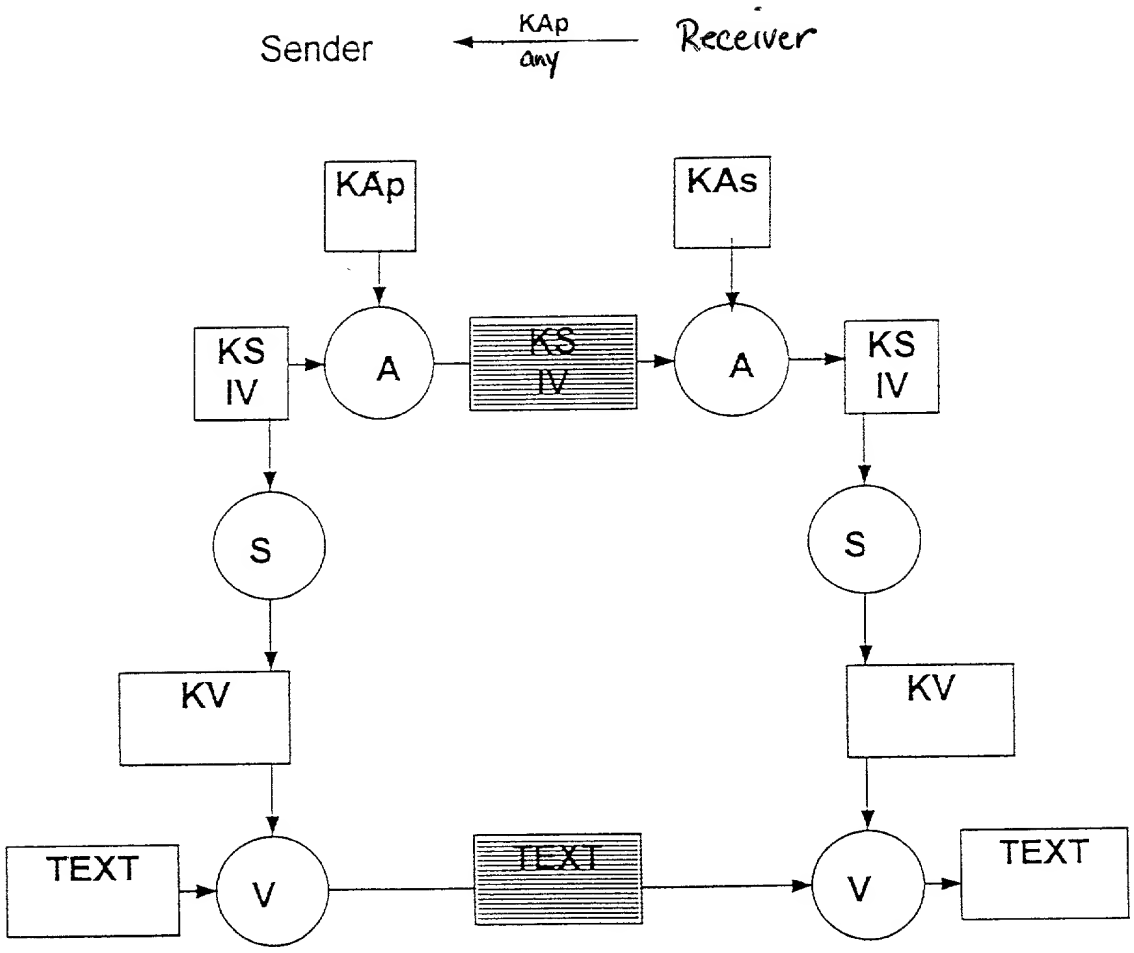

Sender
KAp
any
Receiver
KAp
KAs
KS IV
A
KS IV
A
KS IV
S
S
KV
KV
TEXT
V
TEXT
V
TEXT

FIG. 5

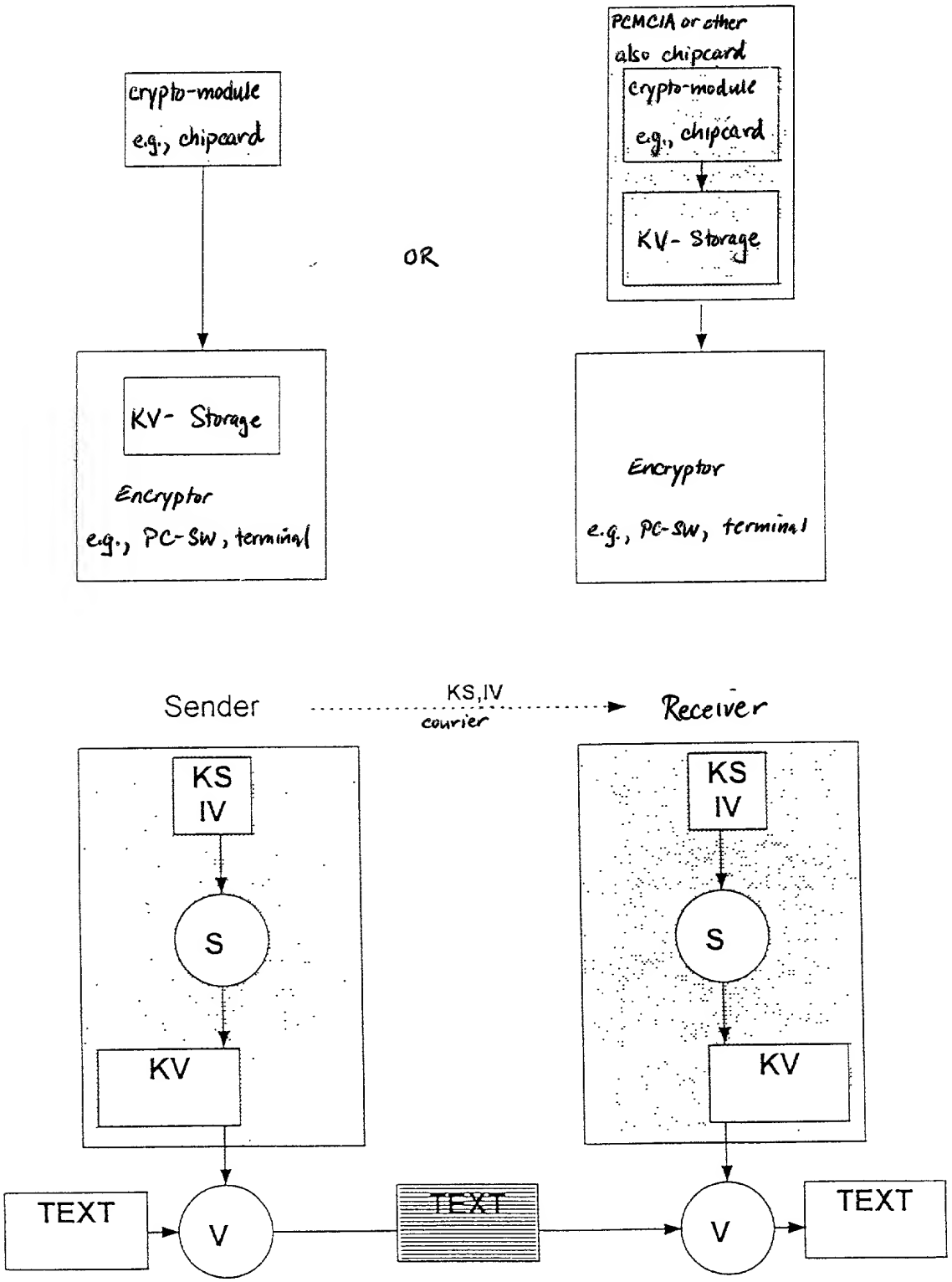
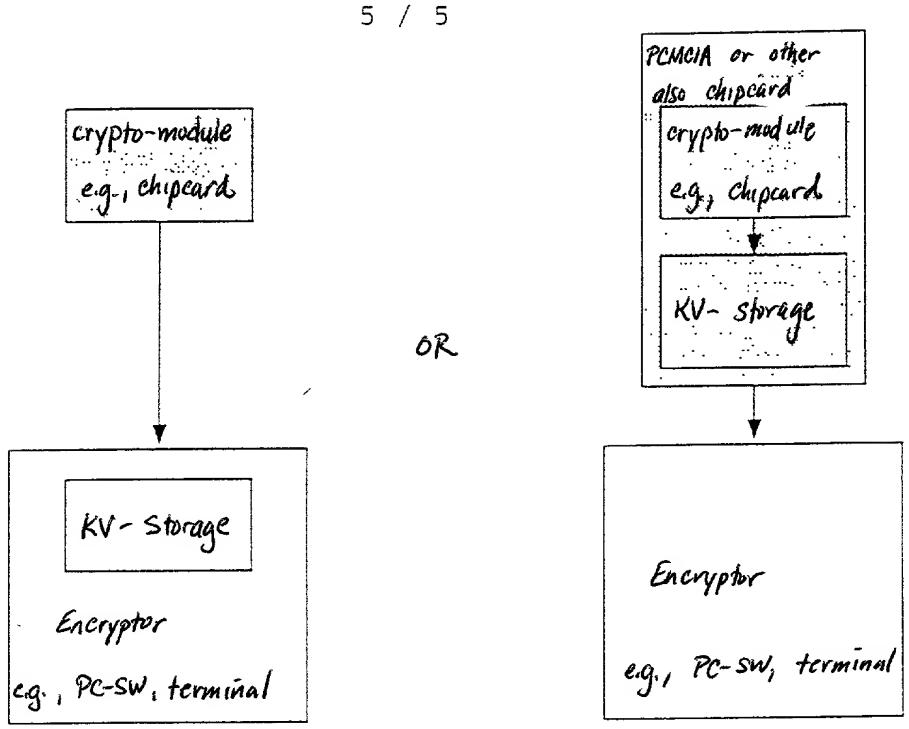

crypto-module
e.g., chipcard
KV- Storage
Encryptor
e.g., PC-SW, terminal
OR
PCMCIA or other
also chipcard
crypto-module
e.g., chipcard
KV- Storage
Encryptor
e.g., PC-SW, terminal
Sender
KS,IV
courier
Receiver
KS
IV
S
KV
TEXT
V
TEXT
KS
IV
S
KV
V
TEXT

FIG. 6


crypto-module
e.g., chipcard
KV- Storage
Encryptor
e.g., PC-SW, terminal
OR
PCMCIA or other
also chipcard
crypto-module
e.g., chipcard
KV- Storage
Encryptor
e.g., PC-SW, terminal

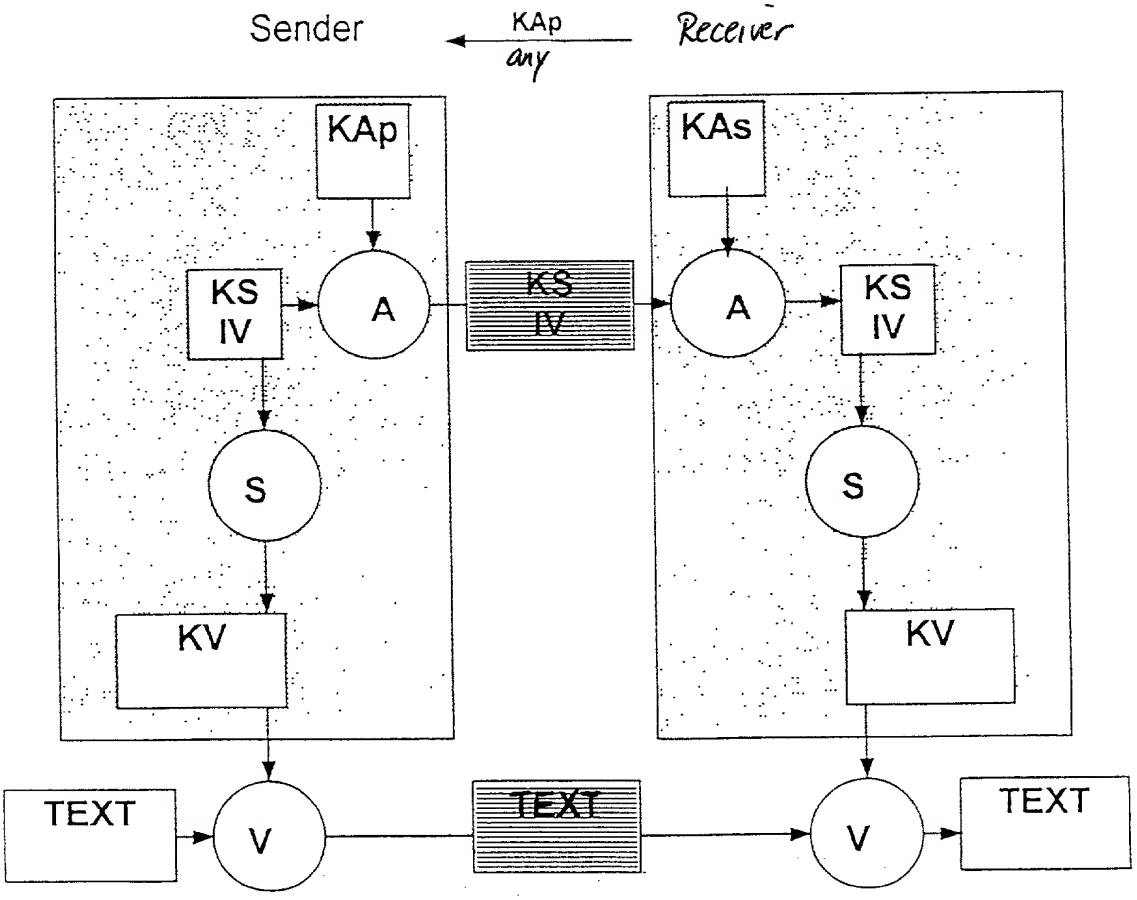

Sender
KAp
any
Receiver
KAp
KS IV
A
KS IV
KS
S
KV
TEXT
V
TEXT
KAs
A
KS IV
S
KV
V
TEXT

FIG. 7

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

# DECLARATION AND POWER OF ATTORNEY

ATTORNEY'S DOCKET NO.
**2345/97**

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name,

I believe I am an original, first, and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled **ENCRYPTION METHOD AND DEVICE**, the specification of which was filed as International Application No. PCT/EP98/01391, on March 11, 1998.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

PRIOR FOREIGN APPLICATION(S)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

| COUNTRY | APPLICATION NUMBER | DATE OF FILING (day, month, year) | DATE OF ISSUE (day, month, year) | PRIORITY CLAIMED UNDER 35 U.S.C. § 119 |
|---|---|---|---|---|
| **GERMANY** | **197 16 861.2** | **22/04/97** | | **YES** |

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys:
**Richard L. Mayer (Reg. No. 22,490)**
**Erik R. Swanson (Reg. No. 40,833)**

SEND CORRESPONDENCE, AND DIRECT TELEPHONE CALLS TO:
**Richard L. Mayer**
**KENYON & KENYON**
**One Broadway**
**New York, New York 10004**
**(212) 425-7200 (phone)**
**(212) 425-5288 (facsimile)**

EL179668975US

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

| | | | |
|---|---|---|---|
| FULL NAME OF INVENTOR 1 of 2 | FAMILY NAME<br>**Kowalski** | FIRST GIVEN NAME<br>**Bernd** | SECOND GIVEN NAME |
| RESIDENCE & CITIZENSHIP | CITY<br>**57072 Siegen** | STATE & ZIP CODE/OR FOREIGN COUNTRY<br>**Germany** DEX | COUNTRY OF CITIZENSHIP<br>**Germany** |
| POST OFFICE ADDRESS | POST OFFICE ADDRESS<br>**Am Bastenberg 4** | CITY<br>**57072 Siegen** | STATE & ZIP CODE/COUNTRY<br>**Germany** |
| Signature | | Date 12th August 1999 | |
| FULL NAME OF INVENTOR 2 of 2 | FAMILY NAME<br>**Wolfenstetter** | FIRST GIVEN NAME<br>**Klaus-Dieter** | SECOND GIVEN NAME |
| RESIDENCE & CITIZENSHIP | CITY<br>**64673 Zwingenberg-Rodau** | STATE & ZIP CODE/OR FOREIGN COUNTRY<br>**Germany** DEX | COUNTRY OF CITIZENSHIP<br>**Germany** |
| POST OFFICE ADDRESS | POST OFFICE ADDRESS<br>**Neckarstr. 19** | CITY<br>**64673 Zwingenberg-Rodau** | STATE & ZIP CODE/COUNTRY<br>**Germany** |
| Signature | | Date | |

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

| | | | |
|---|---|---|---|
| FULL NAME OF INVENTOR | FAMILY NAME<br>**Kowalski** | FIRST GIVEN NAME<br>**Bernd** | SECOND GIVEN NAME |
| RESIDENCE & CITIZENSHIP | CITY<br>**57072 Siegen** | STATE & ZIP CODE/OR FOREIGN COUNTRY<br>**Germany** | COUNTRY OF CITIZENSHIP<br>**Germany** |
| POST OFFICE ADDRESS | POST OFFICE ADDRESS<br>**Am Bastenberg 4** | CITY<br>**57072 Siegen** | STATE & ZIP CODE/COUNTRY<br>**Germany** |
| Signature | | Date | |

| | | | |
|---|---|---|---|
| FULL NAME OF INVENTOR | FAMILY NAME<br>**Wolfenstetter** | FIRST GIVEN NAME<br>**Klaus-Dieter** | SECOND GIVEN NAME |
| RESIDENCE & CITIZENSHIP | CITY<br>**64673 Zwingenberg-Rodau** | STATE & ZIP CODE/OR FOREIGN COUNTRY<br>**Germany** | COUNTRY OF CITIZENSHIP<br>**Germany** |
| POST OFFICE ADDRESS | POST OFFICE ADDRESS<br>**Neckarstr. 19** | CITY<br>**64673 Zwingenberg-Rodau** | STATE & ZIP CODE/COUNTRY<br>**Germany** |
| Signature | | Date Aug 10 99 | |